

Id AF



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 09/898,365
Applicants : Poo, Teng Pin and Lim, Lay Chuan
Filed : July 3, 2001
Art Unit : 2133
Examiner : Gelagay, Shewaye
Confirm. No. : 4356

Docket No. : 1601457-0007
Customer No. : 007470

Mail Stop **Appeal Brief – Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Mailing

I hereby certify that this paper is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date below.

Date: 10/01/08

By: 
Christina Ishihara

REPLY BRIEF

This is a reply brief pursuant to 37 C.F.R. § 41.41 in response to the Examiner's Answer, dated August 1, 2008, in the above-identified application. The rejected claims are reproduced in Appendix A.

Appellants believe that there is no fee for filing this reply brief. However, the Commissioner is hereby authorized to charge any required fees in connection with this reply brief to White & Case's Deposit Account No. 50-3672.

GROUND OF REJECTION TO BE REVIEWED

1. The rejection of claims 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 17, 18, and 20 as unpatentable under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,088,802 (hereinafter “Bialick”).
2. The rejection of claims 6, 12, 16, 19, and 22 as unpatentable under 35 U.S.C. § 103(a) over Bialick.
3. The rejection of claims 3 and 9 as unpatentable under 35 U.S.C. §103(a) over Bialick in view of U.S. Patent No. 6,799,275 (hereinafter “Bjorn”).
4. The rejection of claims 23 and 24 as unpatentable under 35 U.S.C. §103(a) over Bialick in view of U.S. Patent No. 6,385,667 (hereinafter “Estakhri”).

ARGUMENT

1. Rejection of claims 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 17, 18 and 20

The Examiner maintains the rejection of claims 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 17, 18, and 20 under 35 U.S.C. § 102(e) as being anticipated by Bialick. Appellants respectfully traverse.

Independent claims 1, 7 and 17

Claim 1 recites “a biometrics-based authentication module” wherein “access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user’s identity and wherein access to the non-volatile memory is denied to the user otherwise.” Claim 7 recites that “the microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication

module.” Claim 17 recites a step of “denying the user access to the non-volatile memory provided that a match is not identified.”

The Examiner maintains in his Answer that Bialick anticipates or renders obvious these limitations. However, in the Examiner’s Response to Appellants’ Argument at page 14 of the Answer, the Examiner largely disregards the grounds he previously asserted to deny the patentability of the present claims. Nowhere in the Examiner’s Answer does he contradict the arguments that Appellants made in the Appeal Brief.

Instead, the Examiner raises a new argument in an effort to anticipate or render obvious the claimed invention. For the first time, the Examiner references that Bialick discloses that an access code can be used to “identify a ‘personality’” of the user in an effort to render the claimed invention not patentable. Answer at page 15 (“Bialick teaches that a user must successfully enter an acceptable access code (biometrics), not only to control access to the security or other functionality of the peripheral device, but also to identify a ‘personality’ of the user that is stored in the memory of the peripheral devicer [sic]”). The Examiner refers to col. 10 lines 62-67 and col. 11 lines 1-10 from Bialick to support this assertion:

Advantageously, an access code can be used not only to control access to the security (or other) functionality of the peripheral device, but also to identify a "personality" of the user. Each personality is represented by data that establishes certain characteristics of operation of the peripheral device, such as, for example, restrictions on operation of the peripheral device (e.g., limitations on the types of security operations that can be performed) or specification of operating parameters or characteristics (e.g., cryptographic keys or specification of a particular incarnation of a type of security algorithm, such as a particular encryption algorithm). A single user can have multiple personalities: each personality might, for example, correspond to a different capacity in which a user acts. Data representing personalities and corresponding user access codes can be stored in a memory device of the peripheral device.

10

However, the disclosure of using an access code "to identify a 'personality'" in Bialick does not anticipate or render obvious the claimed invention of using biometric authentication to block or allow user access to non-volatile memory. The Examiner makes a number of errors in relying on this teaching. First, Bialick nowhere discloses, teaches, or suggests that biometric authentication can be used as an access code used to identify a personality. In fact, the access code used to identify a personality in Bialick cannot be provided by biometric authentication. Moreover, the Examiner asserts that Bialick discloses that a user with a proper access code is given access to the personality data. This is incorrect as it runs counter to the express teaching of Bialick. These errors are further described below.

The Examiner's assumption that biometric authentication can be used to identify a "personality" is erroneous as it is contrary to Bialick's disclosure. As the portion of Bialick's disclosure above describes, a personality "establishes certain characteristics of operation of the peripheral device, such as, for example, restrictions on operations of the peripheral device (e.g., limitations on the types of security

operations that can be performed) or specification of operating parameters or characteristics (e.g., cryptographic keys or specification of a particular incarnation of a type of security algorithm, such as a particular encryption algorithm).” Thus the personality of the peripheral device depends on the access code entered. Bialick teaches that the peripheral device may have multiple “personalities” that define the operation of the device. In the excerpt above Bialick further discloses that a “single user can have multiple personalities: each personality might, for example, correspond to a different capacity in which a user acts.” This cannot be accomplished if a biometric marker is used as the access code. Biometric authentication is based on unique physical characteristics of a user. While a user can be assigned any number of passwords, a user has only one biometric marker. Therefore, biometric authentication cannot support a single user having multiple “personalities.” Nowhere does Bialick describe, teach, or suggest how a fingerprint or other biometric marker may be used to identify multiple “personalities” of a single user. Bialick’s disclosure of “personalities” does not anticipate or render obvious user access to non-volatile memory based on biometric authentication.

The Examiner also asserts that Bialick discloses that identification of a “personality” allows the user to access the “personality” data. The Examiner then refers to Bialick’s disclosure that “data representing personalities and corresponding user access codes can be stored in a memory device of the peripheral device.” *See* col. 11, lines 8-10. Nowhere does Bialick suggest that the user can have access to the personality data. It would be contrary to Bialick for the user to be able to access this data. Such access would allow the user to alter his or her own personality data or even

alter the access code entered in the first place. This would defeat whatever protections the personality data offered. Also, Bialick does not disclose, teach, or suggest that such access should be limited to the personality data and access code of the authenticated user. Under the Examiner's reading of Bialick, a user could use an access code to gain access and alter any user's access code and the corresponding personalities of the device. Such results run counter to Bialick. Bialick does not teach that identification of a "personality" allows any user access to non-volatile memory. Therefore, Bialick cannot anticipate or render obvious user access to non-volatile memory controlled by biometric authentication.

Finally, on page 16 of his Answer, the Examiner raises the argument that Bialick discloses "that once an acceptance access code has been entered (i.e. authentication using biometrics), the user is enabled to select one of the three modes which includes a target functionality (i.e. to store data in compact flash memory; col. 13, lines 27-49)." In addition to Appellants' previous arguments set forth in their Appeal Brief concerning the myriad of assumptions the Examiner makes that are unsubstantiated in Bialick's disclosure, Appellants also argue that the Examiner conveniently overlooks col. 14, lines 10-19, which disclose biometric authentication only as a target functionality. As argued in the Appeal Brief, Appellants point out again that Bialick discloses no mode in which multiple target functionalities may be used. Bialick simply does not disclose or render obvious biometric authentication controlled access to non-volatile memory, despite the Examiner's desire to read bits and pieces of Bialick more broadly than that specification can support.

Bialick does not disclose all of the limitations of claims 1, 7, and 17 since Bialick does not teach or make obvious controlled user access to non-volatile memory via biometric authentication. Thus claims 1, 7, and 17 are not anticipated or made obvious by Bialick and are in condition for allowance.

Dependent claims 2, 4, 5, 8, 10, 11, 13, 14, 18, and 20

Claims 2, 4, 5, 8, 10, 11, 13, 14, 18, and 20 depend from one of independent claims 1, 7 and 17, and are therefore allowable for at least the same reasons.

2. Rejection of claims 6, 12, 16, 19, and 22

The Examiner maintains the rejection of claims 6, 12, 16, 19 and 22 under 35 U.S.C. § 103(a) as being unpatentable over Bialick. Appellants respectfully traverse.

Claims 6, 12, 16, 19, and 22 depend from one of claims 1, 7, and 17, and are therefore allowable for at least the same reasons.

Claims 6 and 16 recite that the “microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.” Claim 22 recites a step of “providing the user with a bypass authentication procedure provided that a match is not identified.” Bialick does not disclose a microprocessor that provides a bypass mechanism for authentication when authentication by a biometrics-based authentication module fails, and does not disclose providing a bypass authentication procedure provided that a match is not identified. The Examiner has not identified any prior art reference that discloses a bypass mechanism or a bypass authentication procedure for authentication when a biometrics-based authentication fails.

In the Answer, the Examiner argues that it would have been obvious to modify Bialick to include a microprocessor configured to provide a bypass mechanism because “a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by Bialick, in order to provide a system that allows access to the peripheral device without biometric-based authentication in the event that the user incorrectly or incompletely applies security operations,” citing to col. 8, lines 33-37. Here again the Examiner is ignoring the clear disclosure in Bialick that authentication using a biometric device is a target functionality, not a security functionality.

Col. 8, lines 33-37 states:

enable desired interaction with a security device), the possibility that a user will use the system incorrectly (e.g., fail to apply security operations to an interaction with the host computing device, or apply the security operations incor-
5 rectly or incompletely) is reduced.

Though, as shown in FIG. 6, the peripheral device 602 includes security functionality 611 and target functionality

This portion of Bialick discusses a failed or incomplete security operation. Since authentication using a biometric device is a target functionality of Bialick’s peripheral device, this disclosure regarding security operations is not relevant to the biometric device of Bialick. There is nothing in Bialick that teaches or suggests a bypass mechanism for authentication when a biometrics-based authentication fails.

As explained in the Appeal Brief, Appellants’ specification identifies an example of a situation in which the claimed bypass mechanism can be used: a malfunction of verification module 12b. In the event of a biometrics-based authentication module malfunction, the bypass mechanism can enable an authorized

user to gain access to the data stored in the memory of the portable device until the module is repaired. *See* specification, pp. 13-14. Bialick identifies no such situation, and does not teach or suggest that there is any need to deal with a malfunction of a biometrics-based authentication. Bialick does not teach or suggest using an additional user authentication mechanism when a biometrics-based authentication fails. Thus claims 6, 16, and 22 are not obvious in view of Bialick and are in condition for allowance.

Claim 12 recites that “the biometrics-based authentication module is further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory.” Claim 19 recites that “the registered biometrics marker is stored in an encrypted format.”

In the Answer, the Examiner stated that it would have been obvious to one of ordinary skill in the art to modify Bialick “to enhance the security of the library of biometrics data stored in the peripheral device.” The Examiner cites to col. 10, lines 33-36, which discloses that if the *target functionality* is a memory device, then it may be desirable to ensure that unencrypted data cannot be stored in the memory device either inadvertently or on purpose. The phrase “inadvertently or on purpose” requires a state of mind, thus the storing the data on the memory is done by the user. The Examiner also cites to col. 14, lines 53-58, which discloses that a library of biometric data can be stored in a memory device of the peripheral device.

Bialick clearly discloses that use of a biometric device is a *target functionality*, and also clearly discloses that storing data in a memory of the peripheral device by the user is also a *target functionality*. As set forth in the Appeal Brief regarding claims 1,

7, and 17, Bialick does not disclose that the peripheral device is able to embody two different target functionalities at one time. Bialick does not disclose that a user can access the library of biometric data and does not disclose that such a library is encrypted. The disclosure that one target functionality (use of the peripheral device as a memory device) may involve encrypted data does not teach or suggest that another, different target functionality (use of a biometrics device to enter an access code) involves encrypted data.

There is no teaching or suggestion in Bialick to modify a biometrics-based authentication to encrypt a first biometrics marker before storing the first biometrics marker in the non-volatile memory of a portable device. Thus claims 12 and 19 are not obvious in view of Bialick and are in condition for allowance.

3. Rejection of claims 3 and 9

The Examiner maintains the rejection of claims 3 and 9 under 35 U.S.C. § 103(a) as being unpatentable over Bialick in view of Bjorn. Appellants respectfully traverse.

Claims 3 and 9 depend from claims 1 and 7, respectively, and are therefore allowable for at least the same reasons. Further, claims 3 and 9 are allowable over Bialick in view of Bjorn because these references, either alone or in combination, do not teach or disclose all the limitations of claims 3 and 9.

Claim 3 recites a “USB plug for coupling the portable device directly to a USB socket of another USB-compliant device.” Claim 9 recites a “USB device controller coupled to the bus and a USB plug coupled to the bus, such that the portable device is capable of being coupled directly to a USB socket of . . . a host platform.”

In the Answer, the Examiner states that the peripheral device of Bialick is embodied as a card that can be inserted into a slot of a host computer, and argues that this teaches directly coupling the peripheral device to the host computer. While a card such as a PCMCIA card can be directly coupled to a host computer, as the Examiner acknowledges Bialick does not disclose a USB connector. The Examiner then stated that Bjorn teaches a device with a data bus that conforms to a USB standard (col. 2, lines 59 and 60). But as Appellants explained in the Appeal Brief, the discussion in Bjorn about a device having a bus conforming to a USB standard that can receive digital images does not teach or suggest a portable device that has a USB connector that enables the portable device to be coupled directly to a USB socket of another USB-compliant device. Bjorn teaches coupling devices such as a display, a keyboard, and a mouse to a computer system that has a USB bus (col. 2, line 64 – col. 3, line 10), but does not teach or suggest *directly coupling* a USB plug of a portable device having a non-volatile memory to a USB socket of a USB-compliant device. The only portable device of Bjorn that includes a memory is a smart card, which has a size and shape similar to a plastic credit card (col. 1, lines 16-18). A smart card physically cannot support a USB plug. Bjorn does not disclose that the smart card can be directly coupled to the USB bus 310 because Bjorn discloses that the smart card is connected to bus 310 via a smart card receiver 365 (FIG. 3). Thus Bjorn does not disclose, teach, or suggest coupling a portable device having a USB plug directly to a USB socket of a USB-compliant device.

Bialick and Bjorn, either alone or in combination, do not teach or suggest all of the limitations of claims 3 and 9. Thus claims 3 and 9 are not obvious in view of the cited references and are in condition for allowance.

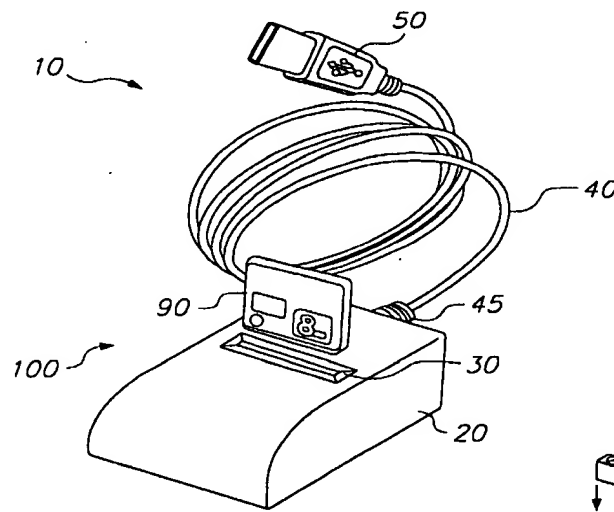
4. Rejection of claims 23 and 24

The Examiner maintains the rejection of claims 23 and 24 under 35 U.S.C. § 103(a) as being unpatentable over Bialick in view of Estakhri. Appellants respectfully traverse.

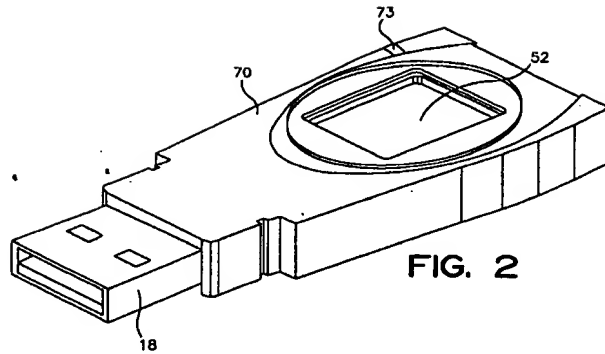
Claim 23 recites a “fingerprint module” and a “memory . . . configured to store at least one fingerprint template as well as user data.” As set forth in the Appeal Brief regarding claims 1, 7, and 17, Bialick discloses that both a biometrics-based authentication and storing data in memory by a user are both *target functionalities*, and that Bialick does not disclose that the peripheral device can embody two different target functionalities at one time. Thus Bialick does not disclose a portable device having both a fingerprint module and a memory configured to store user data.

Claim 23 also recites “a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable storage device directly to a USB socket on a host computer.” In the Answer, the Examiner argues that Estakhri teaches a flash memory card that can be used with different interfaces such as a Universal Serial mode and PCMCIA. But as Appellants pointed out in the Appeal Brief, Estakhri does not teach a USB plug integrated into the housing of a portable memory device without an intervening cable. Rather, Estakhri teaches an interface system that has a 50-

pin connection as a second end 315 for connection to a removable flash memory card and has a first end 314 to couple the interface system to a host computer (col. 5, lines 18-44). The flash memory card 320 of Estakhri has a 50-pin connection, and does not have a USB plug integrated into its housing. The flash memory card of Estakhri is designed to fit within a PCMCIA socket (see col. 1, lines 56-59), and the relative sizes of such a flash memory card and a USB plug are shown in FIG. 1A of Estakhri, reproduced below. Appellants respectfully submit that a card designed to fit within a PCMCIA socket is not physically capable of supporting a USB plug. Thus Estakhri does not teach or disclose a USB plug that is integrated into the housing of a portable data storage device without an intervening cable as recited in claim 23 and as shown in Figure 2 of Appellants' application, reproduced below.



Estakhri, Figure 1A



Appellants' Patent Application, Figure 2

In the Answer, the Examiner argues that it would have been obvious to one of ordinary skill in the art to combine Bialick and Estakhri to provide a fast bi-directional isochronous transfer of data between an external peripheral device and a host computer at very low cost, as suggested by Estakhri at col. 5, lines 41-43. But as set forth above, the combination of Bialick and Estakhri does not disclose all of the limitations of claim 23. Further, as pointed out in the Appeal Brief, the two references disclose systems geared towards completely opposite objectives. Bialick teaches an access control system that serves to restrict access to information stored in a host computer, whereas Estakhri teaches an interfacing system that facilitates access to information stored in multiple memory cards. Thus, Bialick and Estakhri teach two distinct endeavors that seek to achieve opposite results: restricting access to stored information in a host computer versus facilitating access to stored information in multiple memory devices. Bialick's disclosure does not mention a purpose, result, or the desirability of providing a fast data transfer between the peripheral device and the host computer. The fact that Bialick and Estakhri refer to flash memory and Estakhri refers to the USB protocol does not, without more, make the two references combinable, and the combination of the two references

does not disclose all of the limitations of claim 23. As a result, a skilled artisan would not seek to combine the teachings in Bialick and Estakhri.

Bialick and Estakhri, either alone or in combination, do not teach or disclose all of the limitations of claim 23. Claim 23 is not obvious in view of the cited references and is in condition for allowance.

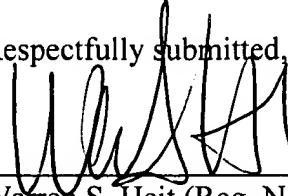
Claim 24 depends from claim 23, and is allowable for at least the same reasons. Further, claim 24 recites that “at least a portion of the USB plug protrudes from the housing to facilitate direct coupling of the unitary portable storage device to the USB socket.” Although the Examiner does not address claim 24 in the Answer, Appellants point out that as set forth above regarding claim 23, Estakhri does not disclose a USB plug integrated into the housing of a portable storage device, so Estakhri cannot disclose that at least a portion of a USB plug integrated into the housing of a portable storage device protrudes from the housing. Bialick and Estakhri, either alone or in combination, do not disclose all of the limitations of claim 24. Claim 24 is not obvious in view of the cited references and is in condition for allowance.

CONCLUSION

For the foregoing reasons, Appellants respectfully submit that the pending claims are not anticipated or obvious in view of the cited references and are in condition for allowance.

Dated: October 1, 2008

Respectfully submitted,



Warren S. Heit (Reg. No. 36,828)
WHITE & CASE LLP
1155 Avenue of the Americas
New York, NY 10036
(650) 213-0321

APPENDIX A: CLAIMS APPENDIX

1. (previously presented) A portable device comprising:
 - a microprocessor;
 - a non-volatile memory coupled to the microprocessor; and
 - a biometrics-based authentication module coupled to and controlled by the microprocessor, wherein access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise.
2. (previously presented) The portable device as recited in Claim 1 wherein the biometrics-based authentication module is a fingerprint authentication module.
3. (previously presented) The portable device as recited in Claim 1 further comprising a universal serial bus (USB) plug for coupling the portable device directly to a USB socket of another USB-compliant device.
4. (previously presented) The portable device as recited in Claim 1 wherein the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the portable device.
5. (previously presented) The portable device as recited in Claim 1 wherein the non-volatile memory comprises flash memory.

6. (previously presented) The portable device as recited in Claim 1 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.
7. (previously presented) A portable device comprising:
- a bus;
 - a microprocessor coupled to the bus;
 - a non-volatile memory coupled to the bus; and
 - a biometrics-based authentication module coupled to the bus, wherein under the control of the microprocessor the biometrics-based authentication module is configured to (1) capture a first biometrics marker; (2) store the first biometrics marker in the non-volatile memory; (3) capture a second biometrics marker; and (4) determine whether the second biometrics marker can be authenticated against the first biometrics marker; and wherein the microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module.
8. (previously presented) The portable device as recited in Claim 7 wherein the biometrics-based authentication module is a fingerprint authentication module.
9. (previously presented) The portable device as recited in Claim 7 further comprising a universal serial bus (USB) device controller coupled to the bus and a USB plug coupled

to the bus, such that the portable device is capable of being coupled directly to a USB socket of and communicating with a host platform via the USB plug.

10. (previously presented) The portable device as recited in Claim 7 wherein the biometrics-based authentication module is structurally integrated with the portable device in a unitary construction and comprises a biometrics sensor being disposed on one surface of the portable device.
11. (previously presented) The portable device as recited in Claim 7 wherein the non-volatile memory comprises flash memory.
12. (previously presented) The portable device as recited in Claim 7 wherein the biometrics-based authentication module is further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory.
13. (previously presented) The portable device as recited in Claim 7 wherein the microprocessor is configured to direct the biometrics-based authentication module to capture and store the first biometrics marker provided that no biometrics marker has been stored in the non-volatile memory.
14. (previously presented) The portable device as recited in Claim 7 wherein the microprocessor is configured to enable access to the non-volatile memory upon a determination of authentication success by the biometrics-based authentication module.

15. (cancelled)

16. (previously presented) The portable device as recited in Claim 7 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.

17. (previously presented) A biometrics-based authentication method implemented using a portable device, the method comprising the steps of:

- (a) obtaining a first biometrics marker from a user with a biometrics sensor installed on the portable device;
- (b) retrieving a registered biometrics marker from a non-volatile memory of the portable device, the registered biometrics marker having been stored therein during a registration process;
- (c) comparing the first biometrics marker against the registered biometrics marker;
- (d) denying the user access to the non-volatile memory provided that a match is not identified in said step (c); and
- (e) signaling an authentication success provided that a match is identified in said step (c).

18. (previously presented) The biometrics-based authentication method as recited in Claim 17 wherein the registered biometrics marker is a fingerprint.

19. (previously presented) The biometrics-based authentication method as recited in Claim 17 wherein the registered biometrics marker is stored in an encrypted format.
20. (previously presented) The biometrics-based authentication method as recited in Claim 17 wherein said step (d) comprises granting the user access to the non-volatile memory.
21. (cancelled)
22. (previously presented) The biometrics-based authentication method as recited in Claim 17 further comprising the step of providing the user with a bypass authentication procedure provided that a match is not identified in said step (c).
23. (previously presented) A unitary portable data storage device having biometrics capability which can be directly plugged into a universal serial bus (USB) socket of a host computer, the device comprising:
- a housing;
 - a fingerprint module, at least a portion of which is housed within the housing, the fingerprint module including a sensor disposed on an exterior surface of the housing;
 - a memory including non-volatile memory, the memory housed within the housing and coupled to the fingerprint module and is configured to store at least one fingerprint template as well as user data;

a memory controller housed within the housing and coupled to the memory, the memory controller controlling access to the memory;

a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer; and

a USB device controller housed within the housing, the USB device controller enabling the unitary portable data storage device to communicate with the host computer via the USB protocol;

wherein the fingerprint module is configured to (1) receive a fingerprint sample from a user placing a finger on the sensor; (2) compare the fingerprint sample with said at least one fingerprint template; and (3) reject a request from the user to access the user data stored in the memory provided that the comparison in said step (2) results in no match.

24. (previously presented) The unitary portable data storage device as recited in Claim 23 wherein at least a portion of the USB plug protrudes from the housing to facilitate direct coupling of the unitary portable data storage device to the USB socket of a computer.

APPENDIX B: EVIDENCE APPENDIX

NONE

, . . .

APPENDIX C: RELATED PROCEEDINGS APPENDIX

NONE